David H. Krieger, Esq.
Nevada Bar No. 9086
HAINES & KRIEGER, LLC
8985 S. Eastern Ave., Suite 350
Henderson, NV 89123
Phone: (702) 880-5554
FAX: (702) 385-5518
Email: dkrieger@hainesandkrieger.com

Matthew I. Knepper, Esq.
Nevada Bar No. 12796
Miles N. Clark, Esq.
Nevada Bar No. 13848
KNEPPER & CLARK LLC
10040 W. Cheyenne Ave., Suite 170-109
Las Vegas, NV 89129
Phone: (702) 825-6060
FAX: (702) 447-8048
Email: matthew.knepper@knepperclark.com
Email: miles.clark@knepperclark.com

Sean N. Payne
Nevada Bar No. 13216
PAYNE LAW FIRM LLC
9550 S. Eastern Ave. Suite 253-A213
Las Vegas, NV 89123
702-952-2733
Fax: 702-462-7227
Email: seanpayne@spaynelaw.com

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

Lynn Marie Cousino, and all similarly situated individuals, Plaintiffs, v. Whole Foods Market, Inc.; Whole Foods Market Group, Inc.; Mrs. Gooch's Natural Food Markets, Inc., and WFM Southern Nevada, Inc., Defendants.	:	Civil Action No.: 17-cv-2531-JAD-PAL **FIRST AMENDED COMPLAINT FOR DAMAGES PURSUANT TO THE FAIR CREDIT REPORTING ACT, 15 U.S.C. § 1681, ET SEQ. AND FOR RELIEF UNDER THE DECLARATORY JUDGMENT ACT, 15 U.S.C. § 2201, AND FOR DAMAGES AND EQUITABLE RELIEF UNDER NEVADA LAW** **JURY TRIAL DEMANDED**

JURISDICTION AND VENUE

1. This Court has federal question jurisdiction because this case arises out of violation of federal law, specifically the Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681(x) ("FCRA"). 28 U.S.C. § 1331; *Smith v. Community Lending, Inc.*, 773 F.Supp.2d 941, 946 (D. Nev. 2011).

2. This Court has supplemental jurisdiction to hear all state law claims under Nevada state law pursuant to 28 U.S.C. § 1367.

3. This Court also has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because the amount in controversy exceeds $5 million exclusive of interest and costs, there are more than 100 putative class members, and at least some members of the proposed Class have different citizenship than Whole Foods.

4. Venue is proper in the United States District Court for the District of Nevada pursuant to 28 U.S.C. § 1391(b) because Plaintiff is a resident of the County of Clark, State of Nevada and because Defendant is subject to personal jurisdiction in the County of Clark, State of Nevada as it conducts business there. Venue is also proper because, the conduct giving rise to this action occurred in Nevada. 28 U.S.C. § 1391(b)(2).

PARTIES

5. Plaintiff Lynn Marie Cousino ("Plaintiff") is a natural person residing in the County of Clark, State of Nevada.

6. Plaintiff and all putative Class members are "consumers" as that term is defined by 15

U.S.C. § 1681a(c). Additionally, Plaintiff and members of the Nevada Subclass are "persons" as used in NRS 598 and NRS 41.600.

7. Defendant Whole Foods Market, Inc. ("Whole Foods Market") is a corporation incorporated under the laws of Texas with its principal place of business in Texas. Whole Foods Market is an indirect wholly-owned subsidiary of Amazon.com, Inc. ("Amazon"). Whole Foods conducts or has conducted business in the State of Nevada through its subsidiaries, including but not limited to WFM Southern Nevada, Inc. ("WFM").[1]

8. On information and belief, it is an indirect subsidiary of Amazon.com, Inc. ("Amazon").

9. Defendant Whole Foods Market Group, Inc. ("Whole Foods Group") is a Delaware Corporation with its principal place of business in Texas. On information and belief, Whole Foods Group conducts or has conducted business in the State of Nevada. On information and belief, it is an indirect subsidiary of Amazon.

10. Defendant Mrs. Gooch's Natural Foods Market, Inc. ("Mrs. Gooch's") is a California corporation with its principal place of business in California. On information and belief, Mrs. Gooch's conducts or has conducted business in the State of Nevada. On information and belief, it is an indirect subsidiary of Amazon.

11. Defendant WFM is a Delaware corporation with its principal place of business in Nevada. On information and belief, it is an indirect subsidiary of Amazon.

[1] *See* Whole Foods Market, Inc. U.S. Securities & Exchange Comm'n, Form 10-k for Fiscal Year Ending Sept. 24, 2107, at 1 ("Whole Foods 2017 10-K"), *available at* https://www.sec.gov/Archives/edgar/data/865436/000086543617000238/wfm10k2017.htm.

12. Defendants Whole Foods Market, Whole Foods Group, Mrs. Gooch's, and WFM are collectively referred to as "Whole Foods Defendants" or "Defendants." Unless otherwise indicated, the use of Whole Foods's name in this Complaint includes all agents, employees, officers, members, directors, heirs, successors, assigns, principals, trustees, sureties, subrogees, representatives, and insurers of Whole Foods.

13. Whole Foods Defendants regularly assemble and/or evaluates consumer credit information for the purpose of furnishing consumer reports to third parties, and uses interstate commerce to prepare and/or furnish the reports. Whole Foods Defendants are "consumer reporting agencies" as that term is defined by 15 U.S.C. § 1681a(f). Additionally, Whole Foods Defendants are "persons" as used in NRS 598 and NRS 41.600, and "Data Collectors" as used in NRS 603A.030.

FACTUAL ALLEGATIONS

Defendants Permit the PII of Numerous Consumers to Be Obtained by Identity Thieves

14. On information and belief, Whole Foods Defendants serve as retailers of natural and organic foods, with approximately 470 stores in North America and the United Kingdom.[2] Certain Whole Foods retail locations also offer taprooms and restaurants. Whole Foods routinely processes consumer transactions at its checkout counters, taprooms, and restaurants through a point-of-sale ("POS") systems which capture personally identifiable information, including names, credit card numbers, card expiration dates, and three-digit security codes located on the back of their credit cards (collectively

[2] *See* Whole Foods 2017 10-k, at 2 ("As of September 24, 2017, we operated 470 stores.").

referred to as "PII").

15. On information and belief, Whole Foods Defendants use different POS systems in their tap rooms and restaurants than they do at their checkout counters.

16. On September 23, 2017, two days prior to the end of Whole Foods Market's fiscal year, the Whole Foods Defendants discovered "unauthorized access of payment card information used at certain venues such as tap rooms and full table-service restaurants located within some stores."[3] This breach included the Whole Foods store at 100 S. Green Valley Pkwy in Henderson, Nevada ("Henderson Whole Foods").[4]

17. Upon information and belief, when Whole Foods Defendants discovered this breach, they began conducting an internal investigation, and engaged third party forensic experts and law enforcement.[5]

18. The fact of the breach was discovered and reported by news organizations on September 28, 2017.[6] According to Defendants, as of October 1, 2017 the breach has impacted approximately 120 stores in 34 U.S. States.[7]

19. For the Plaintiff, as with all potential Class members, these news stories were the first time that they had been specifically informed by Whole Foods Defendants that their

[3] Whole Foods 2017 10-K, at 3.

[4] *See* Whole Foods Market Payment Card Investigation Update ("Whole Foods Update"), available at http://www.wholefoodsmarket.com/customernotification (last visited Dec. 2, 2017).

[5] *See* Imani Moise, *Whole Foods Discloses Data Breach*, Fox Business, Sept. 28, 2017, available at: http://www.foxbusiness.com/features/2017/09/28/whole-foods-discloses-data-breach.html.

[6] *See, e.g.*, Jackie Wattles, *Whole Foods Customer Info Likely Targeted by Hackers*, CNN, Sept. 27, 2017, available at: http://money.cnn.com/2017/09/27/technology/business/Whole Foods-data-breach/index.html.

[7] *See generally* Whole Foods Update (searching for locations by state and city).

information secured by Whole Foods Defendants had been compromised.

20. Between June through September 2017, Plaintiff purchased goods from the Henderson Whole Foods taproom, using a MasterCard or Visa. Whole Foods Defendants, as applicable, processed Plaintiff's consumer transaction with its compromised POS system. Thus, Plaintiff either was or was highly likely to have been implicated in the data breach.

21. As a result, Plaintiff may need to cancel the card she used to complete the transaction and request a new card – an action she would not have to take had her personal information not been likely compromised.

22. Plaintiff, individually and on behalf of those similarly situated, brings this action to challenge the actions of Defendants in the protection and safekeeping of the Plaintiff's and Class members' personal information. Defendants' failures to safeguard consumer PII has caused Plaintiff and Class members damages.

Defendants' Conduct Violated the FCRA.

23. The United States Congress enacted the Fair Credit Reporting Act, 15 U.S.C. § 1681, *et seq.* ("FCRA"), to insure fair and accurate credit reporting, promote efficiency in the banking system, and, as most relevant to this Complaint, protect consumer privacy. The FCRA imposes duties on the CRA's to protect consumer's sensitive personal information.

24. The FCRA protects consumers through a tightly wound set of procedural protections from the material risk of harms that otherwise follow from the compromise of a consumer's sensitive personal information. Through these protections, Congress recognized a consumer's substantive right to protection from damage to reputation,

shame, mortification, and emotional distress that naturally follows from the compromise of a person's identity.

25. Central to the FCRA's privacy protections are restrictions on consumer reporting agencies, or CRAs. A CRA is a person or entity "which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports."

26. Whole Foods is a "consumer reporting agency" ("CRA") within the cognizance of 15 U.S.C. § 1681a(f) because it utilizes a point-of-sale system in which it obtains, evaluates, and/or assembles a consumer's PII in commercial transactions, and directs that PII to be transmitted through a third party credit card processing company and, ultimately, to a financial institution, who then authorizes payment from a consumer's account back to Whole Foods.

27. A central duty that the FCRA imposes upon CRAs is the duty to protect the consumer's privacy by guarding against inappropriate disclosure to third parties. 15 U.S.C. § 1681b codifies this duty, and permits a CRA to disclose a consumer's information only for one of a handful of exclusively defined "permissible purposes." To ensure compliance, CRAs must maintain reasonable procedures to ensure that such third party disclosures are made exclusively for permissible purposes. 15 U.S.C. § 1681e(a).

28. The FCRA defines "consumer report" broadly, as "any written, oral, or other

communication of any information by a CRA bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under section 1681b of this title." 15 U.S.C. § 1681a(d). Under this broad definition, a consumer's PII qualifies as a "consumer report."

29. On information and belief Whole Foods accepts consumer payment for its goods via payment cards issued by members of the payment card industry ("PCI"), such as Visa and MasterCard.

30. Some PCI members founded the PCI Security Standards Council, which developed a Data Security Standard ("DSS") applicable to all merchants that store, process, or transmit cardholder data. In 2009 a Visa official remarked that, "no compromised entity has yet been found to be in compliance with PCI DSS at the time of a breach."[8]

31. PCI members that allow Defendants to process payments through their networks impose several requirements, including the requirement that Defendants fully comply with all of the DSS requirements and individual PCI members' requirements as a condition of being able to process transactions through the PCI members' networks.

[8] Jaikumar Vijayan, *Post-Breach Criticism of PCI Security Standard Misplaced, Via Exec Says*, Computerworld, Mar. 19, 2009, available at: https://www.computerworld.com/article/2531828/security0/post-breach-criticism-of-pci-security-standard-misplaced--visa-exec-says.html.

32. On information and belief, Defendants' failure to protect consumer data from a data breach arose in part from its failure to follow the industry accepted PCI standards. Defendants' actions in designing, implementing, using and/or ratifying the use of the POS system were thus not commercially reasonable insofar as Defendants willfully, or at least negligently, failed to enact reasonable procedures to ensure that the consumer reports accessed through its POS system would only be accessed for a permissible purpose, when in fact they were accessed by data thieves.

33. Defendants failed to properly safeguard the information of Plaintiff and Class members, as required under 15 U.S.C. § 1681e(a). Defendants failed to take the necessary precautions required to safeguard and protect Plaintiff and Class members' PII from unauthorized disclosure, as their PII was improperly handled and stored. Therefore, on information and belief the PII of Plaintiff and Class members was accessed by data thieves and stolen.

Defendants' Conduct Also Violated NRS 598 and NRS 41.600.

34. Between June through September 2017, Plaintiff purchased goods from the Henderson Whole Foods location in the Greater Las Vegas area, using a MasterCard or Visa. Defendants processed Plaintiff's consumer transaction with its compromised POS system. Thus, Plaintiff either was or was highly likely to have been implicated in the data breach.

35. Plaintiff and Class members paid Defendants not only for the goods purchased at their locations, but also for, *inter alia*, the protection of their PII. In so doing, they impliedly

relied on Defendants' promise to keep their PII safe from unauthorized disclosure.

36. Had Plaintiff and Class members known of Defendants' inability to adequately protect PII from unauthorized disclosure, they would have paid substantially less for Defendants' goods, or would have likely "voted with their feet" by purchasing the same goods from another similar seller.

37. However, because Defendants failed to protect Plaintiff and Class members' PII, they did not receive the entirety of the goods they paid for, and correspondingly paid more than they would have otherwise for these goods.

38. Thus, Defendants' conduct also violated NRS 598.0917(7) because it constituted a tender of "goods advertised for sale . . . or tendering terms of sale or lease less favorable than the terms advertised," i.e., goods offered for sale by credit card without the corresponding promise that a consumer's PII would be kept reasonably safe from harm.

39. Defendants also breached their duties under NRS 603A.210, which requires any data collector "that maintains records which contain personal information" of Nevada residents to "implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, . . . use, modification or disclosure." Defendants did not take such reasonable security measures, as shown by a system-wide breach of payment processing systems across approximately 120 stores in 34 U.S. States.

40. Defendants also breached their duties under NRS 603A.215, which requires any data collector doing business in Nevada who accept payment cards in connection with a sale of goods or services to "comply with the current version of the . . . PCI Security

Standards Council . . . with respect to those transactions." On information and belief, Defendants failed to adhere to PCI standards, and was grossly negligent, as it occurred in approximately 120 stores in 34 U.S. States.

41. Additionally, NRS 598.0923(3) provides that a violation of any federal or Nevada law constitutes consumer fraud. Defendant's violations of 15 U.S.C. § 1681e(a), NRS 598.0917(7), and NRS 603A as outlined above, also "relat[ed] to the sale . . . of goods or services," and thus violated NRS 598.0923(3).

42. Defendants' violations of NRS and 598.0923(3), 598.0917(7), and NRS 603A in turn constituted "consumer fraud" for purposes of NRS 41.600(2)(e).

Defendants Breached the Duty of Care They Owed to Their Invitees

43. Defendants routinely engage in commercial transactions in which members of the public, like Plaintiff and Class members, are invited to its business premises to purchase goods.

44. Because Plaintiff and Class members were invitees of Defendants, Defendants owed them a duty of care to inspect for and discover unknown dangers, as well as to notify Plaintiff and Class members of the same.

45. On information and belief, Defendants breached this duty by using a POS system which carried an unreasonable risk that consumer PII would be accessed and stolen, and this risk was never disclosed to Plaintiff and Class members.

Harms Suffered by Plaintiff and Class Members as a Result of the Data Breach.

46. By failing to establish reasonable procedures to safeguard individual consumer's private information, Defendants deprived consumers nationwide from a benefit conferred on

them by Congress under 15 U.S.C. § 1681e(a), which, now lost, cannot be reclaimed. Similarly, Defendants deprived Nevada consumers of a benefit conferred on them by the Nevada legislature in NRS 598 and NRS 41.600, which has been irreparably lost.

47. The harm to Plaintiff and Class members was complete at the time the unauthorized breaches occurred, as the unauthorized disclosure and dissemination of private credit information causes harm in and of itself.

48. Moreover, there is a high likelihood that significant identity theft and fraud has not yet been discovered or reported, and that Plaintiff and Class members' PII will be offered for sale or actually sold in "dark web" marketplaces. This will result in ongoing harm to Plaintiff and members of the Class as data thieves invariably seek to utilize the PII, or seek to re-sell it. Thus, Defendants' wrongful disclosure of Plaintiff and Class members' PII placed them in an imminent, immediate, and continuing risk of harm for identity theft and identity fraud.

49. Plaintiff and Class members have additionally been harmed as they have (1) been forced to take steps to protect against unauthorized disclosures of their PII, (2) incurred, intend to incur, and/or considered incurring the cost of obtaining replacement credit cards, and (3) overpaid for Defendants' goods insofar as a portion of the purchase price was premised on Defendants' implied promise to maintain the security and privacy of Plaintiff and Class Members' PII.

50. Plaintiff and Class members have been obligated to retain an attorney to prosecute this case, and are entitled to an award of reasonable attorney's fees and costs.

CLASS ALLEGATIONS

51. Plaintiff brings this action pursuant to 15 U.S.C. § 1681e(a), on behalf of a nationwide class of all similarly situated individuals ("Class"), defined as:

> All persons in the United States for whom Defendants stored private, personal information that was released as a result of the Whole Foods data breach disclosed in September 2017.
>
> Excluded from the Class are: (1) Defendants, Defendants' agents, subsidiaries, parents, successors, predecessors, and any entity in which Defendants have a controlling interest, and those entities' current and former employees, officers, and directors; (2) the Judge to whom this case is assigned and the Judge's immediate family; (3) any person who executes and files a timely request for exclusion from the Class; (4) any persons who have had their claims in this matter finally adjudicated and/or otherwise released; and (5) the legal representatives, successors and assigns of any such excluded person.

52. Plaintiff also brings this action pursuant to NRS 41.600 and NRS 598.0923(3) on behalf of a subclass of all similarly situated individuals in Nevada ("Subclass"), defined as:

> All persons in Nevada for whom Defendants stored private personal information that was released as a result of the Whole Foods data breach disclosed in September 2017.
>
> Excluded from the Class are: (1) Defendants, Defendants' agents, subsidiaries, parents, successors, predecessors, and any entity in which Defendants have a controlling interest, and those entities' current and former employees, officers, and directors; (2) the Judge to whom this case is assigned and the Judge's immediate family; (3) any person who executes and files a timely request for exclusion from the Class; (4) any persons who have had their claims in this matter finally adjudicated and/or otherwise released; and (5) the legal representatives, successors and assigns of any such excluded person.

53. At this time Plaintiff does not know the size of the Class because the information is exclusively in the possession of the Defendants, but Plaintiff believes that the potential number of Class members is so numerous that joinder would be impracticable.

54. It has been reported that the breach occurred in approximately 120 stores in 34 U.S. States. Given the considerable volume of sales regularly conducted by Defendants at their Whole Foods stores, the Class likely numbers in the millions, if not more. The number of Class members can be determined through discovery, particularly investigation of Whole Foods's internal records.

55. All members of the Class have been subject to and affected by a uniform course of conduct in that all Class members' personal information was compromised during the data breach. These are questions of law and fact common to the proposed Class that predominate over any individual questions. The questions common to all Class and/or Subclass members include, but are not limited to:

a. Whether Defendants had implemented reasonable procedures to ensure that all third parties who accessed Plaintiff's and Class members' private credit information did so for a permissible purpose;

b. Whether Defendants engaged in consumer fraud by violating either NRS 598.0917(7) or NRS 603A with respect to Plaintiff and Subclass members;

b. Whether Plaintiff and Class members suffered damages as a result of Defendants' failure to comply with FCRA and NRS 41.600 based on the improper dissemination of their credit information as a result of the data breach;

c. Whether Plaintiff and Class members are entitled to statutory damages; and

d. Whether Plaintiff and Class members are entitled to punitive damages.

56. Plaintiff's claims are typical of the class, as Plaintiff's PII was compromised during the data breach. All claims are based on the same legal and factual issues.

57. Plaintiff will adequately represent the interests of the class and do not have an adverse interest to the class. If individual class members prosecuted separate actions it may create a risk of inconsistent or varying judgments that would establish incompatible standards of conduct. A class action is the superior method for the quick and efficient adjudication of this controversy. Plaintiff's counsel has experience litigation consumer class actions.

58. Further, under Fed. R. Civ. Pro. 23(a), Defendant acted on grounds generally applicable to the proposed Class, making appropriate final declaratory and injunctive relief with respect to the proposed Class as a whole.

COUNT ONE: VIOLATION OF 15 U.S.C. § 1681, *et al.*
Plaintiff and the Class

59. This Count is brought on behalf of the nationwide Class.

60. Based upon Defendants' failure to have reasonable procedures in place as required by 15 U.S.C. § 1681e(a), Plaintiff's PII was compromised.

61. As a result of each and every willful violation of FCRA, Plaintiff and Class members are entitled to: actual damages, pursuant to 15 U.S.C. § 1681n(a)(1); statutory damages, pursuant to 15 U.S.C. § 1681n(a)(1); punitive damages, as this Court may allow, pursuant to 15 U.S.C. 1681n(a)(2); and reasonable attorneys' fees and costs pursuant to 15 U.S.C. § 1681n(a)(3).

62. As a result of each and every negligent non-compliance of the FCRA, Plaintiff and Class members are also entitled to actual damages, pursuant to 15 U.S.C. § 1681o(a)(1); and reasonable attorney's fees and costs pursuant to 15 U.S.C. § 1681o(a)(2) from Defendant.

COUNT TWO: DECLARATORY JUDGMENT
Plaintiff and the Class

63. At all relevant times, there was in effect the Declaratory Judgment Act ("DJA"), 8 U.S.C. § 2201(a), which states, in relevant part:

> In a case of actual controversy within its jurisdiction . . . any court of the United States, upon the filing of an appropriate pleading, may declare the rights and other legal relations of any interested party seeking such declaration, whether or not further relief is or could be sought. Any such declaration shall have the force and effect of a final judgment or decree and shall be reviewable as such.
> 28 U.S.C. § 2201(a).

64. Plaintiff and Class members seek an order declaring that Defendants' data security procedures failed to meet the PCI DSS standards, which led to the exposure of Plaintiff and Class Members' PII in the data breach.

65. The controversy presented in this case is definite and concrete, and affects the adverse legal interests of the parties. As a result of the data breach and the release of Plaintiff's and Class members' private personal information, Plaintiff and Class members are at a great risk of having that personal information used by unauthorized individuals.

66. There is an actual controversy between the parties of sufficient immediacy and reality to warrant the issuance of a declaratory judgment because Defendants, on information and belief, are not in compliance with the PCI DSS standards which would have better safeguarded Plaintiff and Class members' PII from unauthorized disclosure, both now

and on an ongoing basis. Consequently, Plaintiff and Class members have been, and will continue to be, caused significant harm.

67. There are no disputed legal and factual issues that the Court would have to resolve in granting Plaintiff's and Class members' request for declaratory relief, as this issue does not affect the merits of Plaintiff's and Class members' claims against Defendants.

68. Based on the foregoing facts, Plaintiff and Class members are entitled to a declaration that Defendants' conduct in permitting the data breach failed to meet the PCI DSS standards.

COUNT THREE: VIOLATION OF NRS 41.600
Plaintiff and the Nevada Subclass

69. This Count is brought on behalf of the Nevada Subclass.

70. Defendants engaged in unfair and unlawful acts and practices by failing to maintain adequate procedures to avoid a data breach, and permitting access to consumer reports by data thieves, for whom Defendants had no reasonable grounds to believe would be used for a proper purpose. Plaintiff and Subclass members relied on Defendants' implied promise of data security when providing their PII to Defendants to purchase Defendants' goods.

71. Defendants' conduct violated NRS 598.0917(7) because it constituted a tender of "goods advertised for sale . . . or tendering terms of sale or lease less favorable than the terms advertised," i.e., goods offered for sale by credit card without the corresponding promise that a consumer's PII would be kept reasonably safe from harm. Defendants' violations

of NRS 598.0917(7) constituted "consumer fraud" for purposes of NRS 41.600(2)(e).

72. Additionally, Defendants' violations of 15 U.S.C. § 1681e(a), NRS 598.0917(7) and NRS 603A also "relat[ed] to the sale . . . of goods or services," and thus violated NRS 598.0923(3). Defendants' violations of NRS 598.0923(3) constituted "consumer fraud" for purposes of NRS 41.600(2)(e).

73. Defendants engaged in an unfair practice by engaging in conduct that is contrary to public policy, unscrupulous, and caused injury to Plaintiff and Subclass members.

74. As a direct and proximate result of the foregoing, Plaintiff and Subclass members have suffered injuries including, but not limited to actual damages, and in being denied a benefit conferred on them by the Nevada legislature.

75. As a result of these violations, Plaintiff and Subclass members are entitled to an award of actual damages, equitable injunctive and declaratory relief, as well as an award of reasonable attorney's fees.

COUNT FOUR: Negligence
Plaintiff and the Nevada Subclass

76. This Count is brought on behalf of the Nevada Subclass.

77. Defendants negligently breached its duty of care to its business invitees by failing to uncover and remedy the known risks which led to the data breach, thereby leading to the dissemination of Plaintiff and Subclass members' PII.

78. Additionally, Defendants failed to inform Plaintiff and Subclass members of this heightened risk of harm.

79. Plaintiff and Subclass members suffered damages as a result of Defendants' breach of its duty of care, and are entitled to an award of actual and punitive damages, as well as an award of reasonable attorney's fees.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, respectfully requests the following relief against Defendants:

A. For an award of actual damages against Defendants for all allegations contained in Count One, Count Three, and Count Four;

B. For an award of statutory damages pursuant to 15 U.S.C. §1681n(a)(1) against Defendants for the allegations contained in Count One for each eligible Class member and the Plaintiff;

C. For an award of punitive damages against Defendants as the Court may allow for the allegations contained in Count One pursuant to 15 U.S.C. 1681n(a)(2), and in Count Four under Nevada common law;

D. For an award of the costs of litigation and reasonable attorneys' fees pursuant to 15 U.S.C. §1681n(a)(3) and 15 U.S.C. §1681o(a)(2) against Defendants for each incident of noncompliance of FCRA alleged in Count One, under NRS 41.600(c) as alleged in Count Three, and under Nevada common law as alleged in Count Four;

E. For an order declaring that Defendants' conduct failed to adhere to the PCI DSS standards, as alleged in Count Two;

F. For a preliminary and permanent injunction prohibiting Defendants from continuing to violate the PCI DSS standards as alleged in Count Three; and

G. For all other relief this Court may deem just and proper**.**

//

//

//

//

JURY DEMAND

Plaintiff hereby requests a trial by jury on all issues so triable.

Dated: December 4, 2017

Respectfully Submitted,

/s/ Miles N. Clark
Matthew I. Knepper, Esq.
Miles N. Clark, Esq.
KNEPPER & CLARK LLC
10040 W. Cheyenne Ave., Suite 170-109
Las Vegas, NV 89129

David H. Krieger, Esq.
HAINES & KRIEGER, LLC
8985 S. Eastern Ave., Suite 350
Henderson, NV 89123

Sean N. Payne
PAYNE LAW FIRM LLC
9550 S. Eastern Ave. Suite 253-A213
Las Vegas, NV 89123

Counsel for the Plaintiff and the Class